

What is claimed:

- Sub
A4
1. A method of establishing a private network community (PNC) among a plurality of clients configured to be linked over one or more of a plurality of communication channels, said method comprising:
 - A. linking to a virtual network generation (VNG) system, having access to said communication channels, and establishing a set of PNC attributes, including establishing a set of client attributes associated with said clients and a set of network attributes;
 - B. accessing a VNG system data store including PNC information related to said plurality of clients and a plurality of network types;
 - C. authenticating each of said clients, as a function of said PNC information; and
 - D. establishing said PNC as a function of said set of PNC attributes, including designating a virtual PNC address for each of said clients and linking said clients as if they were connected via a LAN.
 2. The method according to claim 1 wherein said plurality of clients is operated by a corresponding plurality of users and said data store includes identification information related to said plurality of users.
 3. The method according to claim 1 wherein at least one of said plurality of clients is chosen from a group of network enabled devices comprising:
 - 1) a personal computer;
 - 2) a personal digital assistant;

- 5 3) a mobile cellular telephone;
- 6 4) a network appliance;
- 7 5) a digitally loadable music or video player;
- 8 6) an on-line video game; and
- 9 7) a home appliance.

1 4. The method according to claim 1 wherein at least one of said plurality of
2 communication channels is chosen from a group comprising:

- 3 1) Internet;
- 4 2) a cable network;
- 5 3) metropolitan area networks (MAN);
- 6 4) a power-line network;
- 7 5) a telephone line;
- 8 6) a satellite link; and
- 9 7) wireless networks.

1 5. The method according to claim 1 wherein said client attributes include, for each client:

- 2 1) an identification attribute, identifying said client; and
- 3 2) a PNC address attribute, identifying a network location of said client.

1 6. The method according to claim 1 wherein said network attributes include:

- 2 1) a security management attribute, identifying a network security level to
- 3 which said PNC must adhere.

1 7. The method of claim 1 further comprising:

2 E. selectively disestablishing said PNC in response to a termination event.

1 8. The method according to claim 7 wherein step E includes:

2 1) disassociating each of said designated addresses from said clients.

1 9. The method according to claim 7 wherein said termination event includes one of more
2 of the following:

3 1) issuing a termination command by at least one of said clients to said
VNG system;

4 2) detecting completion of a predefined set of tasks;

5 3) detecting a security violation; and

6 4) lapsing of a termination point in time.

7 10. The method according to claim 1 further comprising:

8 E. modifying said PNC attributes; and

9 F. modifying said client links as a function of said modified PNC attributes.

1 11. The method of claim 1, further comprising:

2 E. sending a packet across said PNC, from a first client to a second client, wherein
3 said sending said packet includes:

4 1) grabbing a packet destined for the virtual network card;

5 2) identifying said packet;

- 6 3) wrapping said packet in a wrapper frame by said first client;
- 7 4) transmitting said packet from said first client and receiving said packet
- 8 by said second client;
- 9 5) unwrapping said packet by said second client, and
- 10 6) injecting said packet into a networking driver interface system of said
- 11 second client, as if said packet was received by a standard network card
- 12 of said second client.

1 12. The method of claim 11 wherein sub-step 4) includes:

- a) sending said packet to a VNG server of said VNG system; and
- b) forwarding said packet by said VNG server to a set of destinations clients, including said second client, associated with said packet.

13. The method of claim 12, wherein said first client implements a first protocol and said second client implements a second protocol, and wherein sub-step 3 includes wrapping said packet in a frame compatible with said first protocol and sub-step b) includes:

- i. unwrapping said packet; and
- ii. re-wrapping said packet in a frame that is compatible with said second protocol.
- iii. transmitting said re-wrapped packet to said second client.

1 14. The method of claim 11, wherein sub-step 3) includes compressing said message

2 according to said network attributes and sub-step 5) includes decompressing of said
3 message.

1 15. The method of claim 11, wherein sub-step 3) includes encrypting said message
2 according to said network attributes and sub-step 5) includes decrypting said message.

1 16. The method of claim 1, wherein said VNG system includes a billing manager, said
2 method further comprising:

3 E. monitoring usage of said PNC by said plurality of devices and generating, as a
4 function of said usage, a corresponding usage bill.

17. The method of claim 1 wherein step B includes:

1) accessing a VNG system Web site.

18. A virtual network generation (VNG) system configured to establish and manage a
plurality of PNCs among a plurality of clients and over a plurality of communication
channels, said VNG system comprising:

4 A. a data store including PNC information related to said clients and a plurality of
5 network types;

6 B. a VNG processing device coupled to said data store, said VNG processing
7 device including:

8 1) an authentication manager, configured to receive, store and selectively
9 authenticate a PNC workgroup of clients from said plurality of clients, as

- 10 a function of a client identification;
- 11 2) a PNC manager, configured to receive and store a set of PNC attributes
- 12 related to a PNC to be established, wherein said PNC attributes identify
- 13 the PNC workgroup and a set of PNC security requirements;
- 14 3) a PNC routing manager, configured to generate a PNC address for each
- 15 client; and
- 16 4) a communication manager, configured to link said clients, as if they
- 17 were connected via a LAN, as a function of said PNC attributes; and
- 18 C. a network interface system coupling said VNG processing device to at least one
- of said plurality of communication channels.
19. A VNG system according to claim 18, further comprising:
- D. a PNC termination manager, configured to selectively terminate said PNC in
- response to a termination event.
20. A VNG system according to claim 19 wherein said termination manager is configured
- to disassociate each of said designated addresses from said clients.
21. A VNG system according to claim 19 wherein said termination event includes at least
- one of the following:
- 1) issuing a termination command by at least one of said clients to said
- VNG system;
- 2) detecting completion of a predefined set of tasks;

3) detecting a security violation; and

4) lapsing of a termination point in time.

22. A VNG system according to claim 18 wherein said plurality of clients is operated by a corresponding plurality of users and said data store includes identification information related to said plurality of users.

23. A VNG system according to claim 18 wherein at least one of said plurality of clients is chosen from a group of network enabled devices comprising:

1) a personal computer;

2) a personal digital assistant;

3) a mobile cellular telephone;

4) a network appliance;

5) a digitally loadable music or video player;

6) an on-line video game; and

7) a home appliance.

24. A VNG system according to claim 18 wherein at least one of said plurality of communication channels is chosen from a group comprising:

1) Internet;

2) a cable network;

3) metropolitan area networks (MAN);

4) a power-line network;

- 5) a telephone line;
- 6) a satellite link; and
- 7) wireless networks.

25. A VNG system according to claim 18 wherein said client attributes include, for each client:

- 1) an identification attribute, identifying said client; and
- 2) a PNC address attribute, identifying a network location of said client.

26. A VNG system according to claim 18, further including:

D. a front end VNG system Web site.

27. A VNG system according to claim 18 wherein said network attributes include:

- 1) a security management attribute, identifying a network security level to which said PNC must adhere.

28. A VNG system according to claim 18 wherein said PNC manager includes configured to:

- a) PNC attribute modifier; and
- b) PNC client link modifier, configured to modify said client links as a function of a set of modified PNC attributes.

29. A VNG system according to claim 18, wherein each client in said PNC includes:

D. a client module configured to wrap packets to be transmitted in a wrapper

3 frame, wherein said wrapper frame is compatible with at least one of said
4 plurality of communication channels and a corresponding communication
5 protocol.

1 30. A VNG system according to claim 18, wherein message traffic within said PNC is
2 encrypted.

1 31. A VNG system according to claim 18, wherein said VNG processing device further
2 includes

- 3 5) a usage monitor configured to monitor usage of said PNC by said plurality of
4 clients and generate corresponding usage information; and
5 6) a billing manager, configured to generate a corresponding invoice, as a function
6 of said usage information.